Host Header Attack

It is common for a web-server to host several applications. These applications are distinguished based on the domain-name. So how would a web server know which page the a user wants to visit? The answer is the host-header. In the host header the domain-name is specified.

Password reset

The host-header ca sometimes be parsed in the code and used for creating links. So if the host-header is used for creating the password reset link it is possible for an attacker to steal the reset-token. The attacker just needs to enter the victims email-address in the password reset field, then intercept the request and change the host-header to some address that the attacker controls. When the victim recieves the password reset link they will click on it, which will direct the link to the attackers site, which enables the attacker to steal the reset token, since it will be stored in the url that the user clicks.

Web Cache Poisining